参考資料２

米国 NSF 及び欧州 Horizon2020 におけるサイバーセキュリティ関連の
ファンディングプログラム概要

2020 年 9 月

米国 NSF（全米科学財団）

コンピュータ・情報に係る科学及び工学（Computer and Information Science and Engineering, CISE）研究分野の以下のプログラムが挙げられる。

■Secure and Trustworthy Cyberspace（SaTC）プログラム
○規模（2019 年 9 月公募要領より）
・年間予算$53M、73 課題採択予定、提案は随時募集。
・うち一番大きいものは、最長 4 年で総額$0.5M 以上$1.2M 以下の Medium タイプで 25 課題。
・NSF データベースには、2013 年から採択課題があり 944 課題が掲載。うち Medium タイプは 205 課題、総額$1M 以上は 51 課題。

○プログラムの概要（公募要領より）
セキュリティとプライバシーの基本を様々な学問分野で研究することは、サイバーシステムの設計・開発・運用、今のインフラの防御、人材育成に根本的に新しい方法を生み出す。
プログラムの目標は、国家科学技術評議会(NSTC)の連邦サイバーセキュリティ研究開発戦略プラン(*)等に沿っており、セキュリティとプライバシーを確保しつつ、サイバーシステムがもたらす社会的・経済的便益の増大を守ることにある。
提案は、一つの学問分野でもよいし、学際的でもよい。また、提案の種類として、通常の研究を行う CORE と呼ばれる種類以外に、存在する研究成果を実用化(practice)に移行させる Transition to Practice（TTP)と呼ばれる種類も用意されている。

(*)「科学的基礎(Scientific Foundations)」の構築が重要として以下の記述あり。
(2016 年 2 月、NSTC)

1. サイバーセキュリティは、今や、ハードウェア、ソフトウェア、ネットワーク、データ、人間、物理世界との融合を含むものとなっている。進展する技術や脅威を織り込むことのできる信頼あるシステムの開発には、発見的手法(heuristic methods)は不適切であり、対症療法的で、不完全で、重要な脆弱性を見逃すことがある。
2. このため、サイバーセキュリティには、明確な目的を持った健全な数学的及び科学的基礎、包括的な理論(例えば、防御、システム、敵対勢力に係るもの)、原理に基づいた設計方法論、マルチスケールでの複雑で動的なシステムのモデル、成否を評価するための指標が必要となる。
3. 科学的に確立されよく理解されている先端の解決策は、様々なセキュリティ分野のサブ領域に不均一にしか存在しない。ほとんどのテクニックは、領域やコンテクストに特有のもので、数学的及び実証的な健全性が検証されておらず、有効性や効率性が考慮されていない。このため、対策の実態は、発見的なテクニック、敵対的行動を推測した非公式な原理やモデル、プロセスに寄った評価基準によるものとなっている。
4. 以下の領域での科学的基礎の構築は重要。1）脅威の量的な定義、計量的なセキュリティの仮定と保証、システム・防御・敵対勢力の構成を評価する効率的で公式化された手法を持ち合わせた、抑止・防護・検知・適応の 4 要素に係る公式なフレームワーク。2）証明及び計量が可能なセキュリティ措置対象の確認・検証を伴う、原理に基づいたデザイン法。3）進展する破壊的な技術及び脅威を予測する推論フレームワーク。

※公募要領：Program Solicitation NSF 19-603, 2019 年 9 月

■Secure and Trustworthy Cyberspace (SaTC) Frontiers プログラム
○規模（2019 年 4 月公募要領より）
・年間予算$15M。最長 5 年で総額$5M から$10M を支援。

○プログラムの概要（公募要領より）
SaTC プログラムの傘の下で、意欲的かつ潜在的に変革的なセンター規模のプロジェクトを支援。1）科学的に深い質問・難問や、説得力ある応用・新規技術に突き動かされた、遠大な研究的探究を行うもの。2）知識の移転を通じて、重要な研究・教育のアウトカムをもたらすもの。

○採択課題（2 件）（上のプログラムの NSF データベースの課題数の内数）
・Security and Privacy in the Lifecycle of IoT for Consumer Environments (SPLICE)
PI: David Kotz, Dartmouth College / 支援期間 2020 年-2025 年、本年$1.1M
スマートホームでの人間、社会的、技術的な挑戦を研究する。1）新しい方法を通じた住人による状況認識、2）プライバシー管理の新しい方法、3）プライバシーに関する全体的な概念フレームワークに取り組むとともに、異なった環境における人的要因の科学的理解を深める。
・Protecting Personal Data Flow on the Internet
PI: Athina Markopoulou, UC Irvine / 支援期間 2020 年-2025 年、本年＄0.86M
学際的な手法でインターネットのデータ流通の透明性と管理を向上させる。広告システムを分権化する IoT アーキテクチャという代替策についても研究する。

※公募要領：Program Solicitation NSF 19-572, 2019 年 4 月

■Cybersecurity Innovation for Cyberinfrastructure (CICI) プログラム
○規模（2018 年 10 月公募要領より）
・年間予算$10M-$19.5M、6-12 課題採択予定。

○プログラムの概要
end-to-end で科学活動のインテグリティ等が確保されるようセキュリティ解決策を開発・展開・統合する。1）セキュアな科学用サイバーインフラ、2）研究データ保護、3）信頼あるサイバーインフラのための COE、が対象。

※公募要領：Program Solicitation NSF 19-514, 2018 年 10 月

出所：NSF ホームページ https://www.nsf.gov/funding/programs.jsp?org=CISE
NSF データベースの情報は 2020 年 8 月末現在

欧州 Horizon 2020（EU 研究・イノベーション枠組み計画）

計画の Excellent Science の柱の下に、分野をとわず研究助成を行う ERC（欧州研究評議会）のファンディングがあり、Computer Science and Informatics 分野に「security, privacy, cryptology, quantum cryptography」のパネルがある。

また、計画の Societal Challenge の柱の下に Secure Societies 分野があり、以下のプログラムが挙げられる。

■Digital Security 公募プログラム（Work Programme 2014-15 より）
○規模　2014 年 €47M、2015 年　€50M
○概要
・本公募の焦点は、研究室でテストされてきた最新のセキュリティ、プライバシー、信頼上の対策の実行可能性と成熟度を実証することにある。
・公募対象の Topics として以下の 7 つ。1）プライバシー（大量データ処理においてプライバシーを保護する手法の研究など）、2）アクセス制御、3）重要インフラ防護における ICT の役割、4）情報ドリブンのサイバーセキュリティマネジメント、5）トラスト e サービス、6）リスクマネジメント及び保証モデル、7）欧州の価値観に配慮したサイバーセキュリティの技術革新

■Digital Security 公募プログラム（Work Programme 2016-17 より）
○規模　2016 年 €64M、2017 年 €56M
○概要
・公募対象の Topics として以下の 8 つ。1）信頼あるセキュアな ICT システム等の保証と認証、2）中小企業等のサイバーセキュリティ（エンドユーザーの状況認識や管理を保ったまま使い勝手よく自動化された革新的な対策を開発する）、3）　医療分野のデジタルセキュリティ増大、4）サイバーセキュリティの経済学、5）EU 協力と国際対話（日米との対話含む）、6）PPP：暗号 、7）PPP：先端的な脅威、8）PPP：プライバシー、データ保護、デジタル本人確認　※注：PPP とは Public-Private Partnership

■Digital Security 公募プログラム（Work Programme 2018-20 より）
○規模　2018 年 €45M、2019 年 €38M、2020 年 €69M
○概要
・公募対象の Topics として以下の 5 つ。1）サイバーセキュリティ準備：サイバーレンジ、シミュレーション、経済学、2）知的なセキュリティ及びプライバシーマネジメント、3）市民と中小企業のデジタルセキュリティ及びプライバシー、4）電力・エネルギーシステムのサイバーセキュリティ、5）重要セクターのデジタルセキュリティ、プライバシー、データ保護、説明責任

さらに、計画の Industrial Leadership の柱の下に ICT 分野があり、以下の公募が挙げられる。

■ICT 公募プログラムのうち ICT Cross-Cutting Activities（Work Programme 2014-15 より）
○規模　ICT 全体の 2014 年 €695M のうち数
○概要
・公募対象の 4 つの Topics の 1 つが「Cybersecurity, Trustworthy ICT」。Topics の範囲としては E2E のセキュリティバイデザイン及び暗号とされている。

出所：Horizon 2020 ホームページ　https://ec.europa.eu/programmes/horizon2020/h2020-sections
Secure Societies 分野の Work Programme 及び ICT 分野の Work Programme より